Victorian Government
Information Security

Inner Budget Agencies Critical Information Infrastructure (CII)

Health Check Template

Template for *Health Check* of Inner Budget (IB) agency CII – SEC STD 02

Keywords:	CII, health check, template	
Identifier: SEC TEMP 02-2	**Version no.:** 1.0	**Status:** Final
Issue date: 16 April 2012	**Date of effect:** 16 April 2012	**Next review date:** 1 July 2014
Owner: Department of Treasury and Finance Victorian Government	**Issuing Authority:** Department of Treasury and Finance Victorian Government	

Background

This *Health Check* is part of the Inner Budget (IB) agency Critical Information Infrastructure (CII) Risk Management (RM) Framework, which is intended to ensure a consistent approach to the prioritisation of activities for the protection of CII assets.

Scope

The scope of this Health Check covers the CII systems of the 15 Inner Budget (IB) departments and agencies, and CenITex (collectively referred to as 'IB agencies' hereafter).

A Health Check is required for each system categorised as belonging to IB CII.

Purpose

The purpose of the CII Health Check report is to communicate the status of high level CII security arrangements to executive management.

It answers the following questions:

- Are the governance arrangements for each CII system adequate?
- How do we need to improve the protection of CII systems?
- Where should we invest in additional risk mitigations?
- Has our risk posture changed on the past 12 months?

Interpretation

What is the *Health Check* report?

The *Health Check* IS NOT a detailed report that identifies and rates each threat and vulnerability and then maps it to a treatment plan. The *Health Check* focuses on the governance, processes, activities and analyses required to identify and assess risks.

What does a negative (Red) or partial response (Yellow) mean?

It indicates that senior management may

- not have adequate information to make an assessment on whether CII assets are secure, or
- have an assurance gap i.e. that all reasonable actions to protect CII assets are NOT in place and/or activities are NOT regularly completed to identify and manage risks to CII assets.

Actions Required as a Result of the Self-Assessment

Agencies should develop and implement a plan to address

- as a first priority, the issues assessed as Red,
- as a second priority the issues assessed Yellow, and
- Compliance Reporting – Refer to SEC STD 02.

IB Agency Name:		Result			*Green* = *currently compliant (this year)* *Yellow* = *last compliant 1-3 years ago* *Red* = *not compliant/ last compliant >3 years ago*
System/CII Asset:		**GREEN**	**YELLOW**	**RED**	**Comments:** If not applicable, put 'n/a' in comments column. You are NOT required to submit original documentation to substantiate your answers. Simply state the document name, date completed, and contact details.
Age of system (years):					
Planned upgrade date:					
Criteria:					
1. Is there a responsible executive and governance committee for this CII asset?		☐	☐	☐	
2. Does this CII asset have a formally documented Owner or Custodian who is responsible for protecting the CII asset?		☐	☐	☐	
3. Are the key threats to the Confidentiality, Integrity and Availability of this CII asset documented and signed off via a *System Risk Management Plan* (SRMP) or equivalent threat and risk analysis?		☐	☐	☐	
4. Has the Confidentiality assessment above resulted in a formal information security classification for this CII asset?		☐	☐	☐	
5. Does this CII asset store personally identifiable data which is subject to the *Information Privacy Act* and/or *Health Records Act*? If so, is a current *Privacy Impact Assessment* in place?		☐	☐	☐	
6. Is there a current, and fully implemented, *System Security Plan* (SSP) or equivalent list of risk mitigations, for this CII asset?		☐	☐	☐	
7. Are sub contractors or third parties engaged to support this CII asset? If so, has each external party been subjected to a formal information security assessment? Do contracts with external parties include ICT Security terms and conditions, including compliance with the PSPF and ISM?		☐	☐	☐	
8. Is there multi agency access to this CII asset and/or is CII data from the CII asset shared with third parties? If so, are formal MOUs in place with all third parties which address access and security requirements including compliance with the PSPF and ISM?		☐	☐	☐	
9. Has web, application and database penetration testing (as applicable) been completed for this CII asset?		☐	☐	☐	
10. Do the CII environments for this asset comply with DSD's *Top Four Mitigation Strategies To Protect Your ICT System* i.e. patching third party applications; patching operating systems; minimising administrative privileges; application whitelisting?		☐	☐	☐	
11. Is there a recently tested *Business Continuity Plan* for all services supported by this CII asset, including an assessment of third party service providers?		☐	☐	☐	
12. Is there a recently tested ICT *Disaster Recovery Plan* for this CII asset, including (where necessary) an assessment of third party service providers?		☐	☐	☐	
13. Is information security for this CII asset continually monitored, and is the security incident response process documented and effective?		☐	☐	☐	
14. Has an independent expert or auditor assessed the adequacy of information security for this CII asset?		☐	☐	☐	